Remote patient monitoring using safe and secure WBAN technology

Neeraj Joshi, Syed Zain Hassan Zaidi, Mohamed Ben Haj Frej

1. Abstract

In the recent years, we have witnessed a tremendous growth and development in the field of wireless communication technology and sensors. Resulting into opening new dimensions in various research fields. The integration of Nano scale devices with low power consumption circuits brought a new evolution in wireless networks. This blend of technologies led to the formation of a new field in WSN (Wireless Sensor Networks) known as WBAN (Wireless Body Area Network). WBAN is based on small sensors designed to operate and function mainly on the human body. As we are dealing with human lives, security and privacy are major concerns as patients' data is at the stakes. Authentication is an important factor in securing information from unauthorized usage. Now-a-days a lot of research has been done in order to improve the overall authentication mechanisms in WBAN. In this poster, we are surveying the security challenges in WBAN with a focus on the authentication phase. A list of several methods along with their schemes has been studied and recapitulated. ECG is one the most popular schemes used in WBAN, benefiting from its uniqueness. However, it comes with challenges as creating an extract trait could get complicated. ECG could be aided by the help of combining fingerprint which will result in a non-destructive method of biometric authentication compared with single ECG trait.

2. Introduction

- Technological advancement in the field of wireless communication and sensors gives rise to a type of network which is known as WBAN (Wireless Body Area Network).
- WBAN made tele medical options more viable by monitoring critical parameters and sending information to remote centralized stations.
- Medical Body Area network consists of small devices which are ultra-low power communicating via wireless network.
- It is actually a communication network which exists between humans and computers and it could be through wearable and implanted BANs
- Some of the challenges which are faced by WBAN is dependability and security

3. WSN vs WBAN

Parameters	WSN	WBAN
Mobility	They usually have stationary nodes.	WBAN nodes are not stationary. Though mobility pattern within WBAN nodes is the same.
Data rate	It is event based monitoring and triggered only when an event occurs and it could happen in an Irregular fashion.	It has a stable and periodic based monitoring system.
Deployment	It is installed in remote places where human access is difficult and it requires extra nodes in order to deliver information in case of node failure.	Nodes are installed on the need basis. So every node is important.

4.Research analysis of Biometric based authentication

Author Name	Year	Problem	Scheme	Result
Lin Yao et al.	2011	Security of WBAN parameters.	ECG based authentication protocol.	Achieved confidentiality of health information by using unique characteristics of an individual.
Wei Wang et al	2010	Key based authentication protocol.	Biometric authentication using uniformed GMM (Gaussian mixture model)	Medical information is secured in WBAN architecture by utilizing IPI signals and statistical based signing process.
Krishna Kumar Venkatasubramanian et al.	2008	Privacy preservation.	Electrocardiogram based key generation.	ECG based keys can be used to secure information between sensors in WBAN.
Sofia Najwa Ramli et al.	2013	Convention of biometric were vulnerable.	Analyzed by combining ICA (Independent component analysis) and frequency component of the ECG signal	ECG signal are uniquely represented making it hard to be forfeited by an intruder.
Chunqiang Hu et al.	2013	Elasticity with the authentication system.	Fuzzy attribute based signcryption method.	Message is also read by group of users who satisfies the certain access control rules under emergency situation.
Zhaoyang Zhang et al.	2012	Integrity of person's medical data over wireless environment.	Improved Jules Sudan (IJS) algorithm is used for authentication.	ECG-IJS is lightweight and energy efficient security solution for WBAN.
Ayan Banerjee et al.	2010	Securing inter-sensors involved in communication within WBAN.	physiological-signal-based key agreement (PSKA)	It is feasible to implement PSKA to get required security in WBAN.
Honggang Wang et al.	2011	Time synchronization and key distribution.	wavelet-domain Hidden Markov Model (HMM)	Successful integration of biometric information in order to enhance security.
Ruggero Donida et al.	2014	Traditional ECG based template had problems.	Use of Binary ECG based template.	Lesser error rate achieved by using Binary ECG based strings in comparison with conventional technique.
Manjunathswamy et al.	2015	Lack of accuracy in existing ECG based biometric approach	Use of multimodal biometric scheme.	Making use of finger print and ECG biometric recognition system in a fusion to get more reliable biometric authentication technique.

5. Data security and Privacy

- Importance of Patient Data and its Security goes hand in hand in WBAN.
- Data security is defined as transferring data on to the network and saving it securely within a database.
- Data privacy is an efficient authentication mechanism which grants access to only legitimate user.
- Major requirements for security and privacy within WBAN can be well defined by analyzing the following terms:
  - *Data Encryption*
  - *Data Integrity*
  - *Data aggregation*
  - *Data availability*
  - *Secure Localization*
  - *Authentication*
  - *Secure management*

6. What is Biometric and how secure is it?

- Biometric techniques authorize a genuine user on successful identification of his or her specific human body possessions.
- One of the authentication types is biometric and it relies on verification by the help of individuals unique intrinsic characteristics.
- Biometric makes a system secure by having parameters such as Permanence, Collectability, Uniqueness, Acceptability, Invulnerability.

7. Recommendations

- Authentication phase is more reliable as hackers have to gain access on more than one biometric modalities to get into highly secured patient data.
- The security of WBAN can be more enhanced by fusion of some of existing biometric techniques such fingerprint, Face recognition, IRIS and DNA.
- Multimodal schemes will prove to be a new era in authentication phase adding advanced capabilities of capturing more than one biometric trait to backup if one fails.

8. Conclusion

This research is an overview of WBAN security related issues lying within its authentication phase. After analyzing a short span of years by different researches to provide best biometric scheme to secure WBAN authentication phase, One of the appropriate methods to expand on would be to utilize multimodal biometric authentication proposed by Manjunathswamy B E et al. WBAN played a key role in providing a more affordable health solution with some great advantages like premature detection which is beneficial for both patients and doctors. WBAN is still in initial phase of development and has some issues and challenges to be addressed especially secutity wise.

9. References

1. Yao, L., et al., *A biometric key establishment protocol for body area networks.* International Journal of Distributed Sensor Networks, 2011. **2011**
2. Wang, W., et al. A stochastic biometric authentication scheme using uniformed GMM in wireless body area sensor networks. in Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on. 2010. IEEE.
3. Venkatasubramanian, K.K., A. Banerjee, and S.K. Gupta. *EKG-based key agreement in body sensor networks*. in *INFOCOM Workshops 2008, IEEE*. 2008. IEEE.
4. Ramli, S.N., R. Ahmad, and M.F. Abdollah. *Electrocardiogram (ECG) signals as biometrics in securing Wireless Body Area Network*. in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*. 2013. IEEE.
5. Hu, C., et al., *Body area network security: a fuzzy attribute-based signcryption scheme.* Selected Areas in Communications, IEEE Journal on, 2013. **31**(9): p. 37-46.
6. Zhang, Z., et al., *ECG-cryptography and authentication in body area networks.* Information Technology in Biomedicine, IEEE Transactions on, 2012. **16**(6): p. 1070-1078
7. Wang, H., et al. *An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)*. in *Communications (ICC), 2011 IEEE International Conference on*. 2011. IEEE.
8. Donida Labati, R., et al. *HeartCode: A novel binary ECG-based template*. in *Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings, 2014 IEEE Workshop on*. 2014. IEEE.
9. Manjunathswamy, B., et al. *Multimodel Biometrics Using ECG and Fingerprint*. in *International Conference on Advances in Communication Network and Computing-CNC, at Chennai, India*. 2014.